CLAIMS

1. An apparatus having a digital protection mechanism, comprising:

a tangible object;

a digital protection system attached to said tangible object, said digital protection system comprising:

(a) an external interface for receiving data requests;

(b) a processor coupled to said external interface, said processor capable of transforming data according to a first public/private key encryption algorithm; and

(c) an internal data storage, said internal data storage storing an identity private key, said identity private key being inaccessible outside said external interface; and

a data descriptor associated with said digital protection system, said data descriptor including an identity public key, attribute data and a digital signature;

wherein said processor performs a first transformation of data responsive to a request received through said external interface, said processor performing said first transformation of said data according to said first public/private key encryption algorithm using said identity private key, wherein a second transformation of data according to said first public/private key encryption algorithm using said identity public key is a complementary transformation of said first transformation.

2. The apparatus of claim 1, wherein said digital signature is an encryption of data derived from said identity public key and attribute data, said encryption being according to a second public/private key encryption algorithm using a signature private key, said digital signature being capable of decoding according to said second public/private key encryption algorithm using a signature public key.

3. The apparatus of claim 2, wherein said digital signature is an encryption of data derived from said identity public key and attribute data by performing a pre-defined hash function.

4. The apparatus of claim 1, wherein said digital protection system is implemented in digital logic contained on a single integrated circuit substrate.

5. The apparatus of claim 4, wherein said data descriptor is stored in said internal data storage contained on said single integrated circuit substrate.

6. The apparatus of claim 1, wherein at least a portion of said data descriptor is stored in data storage external to said external interface of said digital protection system.

7. The apparatus of claim 1, wherein said tangible object is a digital data processing device having at least one processor external to said digital protection system, said processor external to said digital protection system communicating with said digital protection system across said interface.

8. The apparatus of claim 1, wherein said external interface mates with a corresponding interface of a digital data processing device separate from said tangible object.

9. The apparatus of claim 1, wherein at least a portion of said attribute data is encrypted.

10. A method for using verified information concerning a tangible object, comprising the steps of:

accessing descriptor data associated with the tangible object, said descriptor data including an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing information concerning said tangible object, and a digital signature;

verifying that said digital signature matches said identity public key and said attribute data;

performing a pair of complementary data transformations on source test data to produce resultant test data, said pair of complementary data transformations being performed by:

(a) performing a first data transformation according to said first public/private key encryption algorithm using said identity public key, and

(b) accessing a digital protection system attached to said tangible object to perform a second data transformation according to said first public/private key encryption algorithm using an identity private key in said digital protection system, said identity private key corresponding to said identity public key according to said first public/private key encryption algorithm, said second data transformation being complementary to said first data transformation;

comparing said source test data with said resultant test data; and

using said attribute data in a manner dependent on the results of said step of verifying that said digital signature matches said identity public key and said attribute data, and said step of comparing said source test data with said resultant test data.

11. The method for using verified information concerning a tangible object of claim 10, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data according to a derivation algorithm, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein said step of verifying that said digital signature matches said identity public key and said attribute data comprises:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

deriving data from said identity public key and said attribute data using said derivation algorithm; and

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data according to said derivation algorithm.

12. The method for using verified information concerning a tangible object of claim 11, wherein said derivation algorithm comprises a hash function.

13. The method for using verified information concerning a tangible object of claim 11, wherein said derivation algorithm is an identity function which produces as output an identical copy of the input.

14. The method for using verified information concerning a tangible object of claim 10, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation.

15. The method for using verified information concerning a tangible object of claim 10, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

16. The method for using verified information concerning a tangible object of claim 10, wherein said step of accessing descriptor data comprises obtaining said descriptor data from said digital protection system.

17. The method for using verified information concerning a tangible object of claim 10, wherein said source test data is randomly generated data.

18. The method for using verified information concerning a tangible object of claim 10, wherein said tangible object is a digital data processing device having at least one processor external to said digital protection system.

19. The method for using verified information concerning a tangible object of claim 10, wherein said digital protection system of said tangible object includes a coupling for mating with a local digital data processing device separate from said tangible object.

20. A program product for using verified information concerning a tangible object, said program product comprising a plurality of processor executable instructions recorded on signal-bearing media, wherein said instructions, when executed by a processor of a digital data processing device, cause the digital data processing device to perform the steps of:

accessing descriptor data associated with the tangible object, said descriptor data including an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing information concerning said tangible object, and a digital signature;

verifying that said digital signature matches said identity public key and said attribute data;

performing a pair of complementary data transformations on source test data to produce resultant test data, said pair of complementary data transformations being performed by:

(a) performing a first data transformation according to said first public/private key encryption algorithm using said identity public key, and

(b) accessing a digital protection system attached to said tangible object to perform a second data transformation according to said first public/private key encryption algorithm using an identity private key in said digital protection system, said identity private key corresponding to said identity public key according to said first public/private key encryption algorithm, said second data transformation being complementary to said first data transformation;

comparing said source test data with said resultant test data; and

using said attribute data in a manner dependent on the results of said step of verifying that said digital signature matches said identity public key and said attribute data, and said step of comparing said source test data with said resultant test data.

21. The program product for using verified information concerning a tangible object of claim 20, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data according to a derivation algorithm, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein said step of verifying that said digital signature matches said identity public key and said attribute data comprises:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

deriving data from said identity public key and said attribute data using said derivation algorithm; and

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data according to said derivation algorithm.

22. The program product for using verified information concerning a tangible object of claim 21, wherein said derivation algorithm comprises a hash function.

23. The program product for using verified information concerning a tangible object of claim 21, wherein said derivation algorithm is an identity function which produces as output an identical copy of the input.

24. The program product for using verified information concerning a tangible object of claim 20, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation.

25. The program product for using verified information concerning a tangible object of claim 20, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

26. The program product for using verified information concerning a tangible object of claim 20, wherein said step of accessing descriptor data comprises obtaining said descriptor data from said digital protection system.

27. The program product for using verified information concerning a tangible object of claim 20, wherein said source test data is randomly generated data.

28. A method for updating attribute data associated with a tangible object, comprising the steps of:

receiving a request to a service provider from a requestor to update said attribute data, the request including an identity public key for transforming data according to a first public/private key encryption algorithm;

performing a pair of complementary data transformations of source test data to produce resultant test data, a first of said pair of complementary data transformations being performed by said service provider according to said first public/private key encryption algorithm using said identity public key, and a second of said pair of complementary data transformations being performed by requesting a digital protection system attached to said tangible object to perform said second data transformation according to said first public/private key encryption algorithm using an identity private key in said digital protection system, said identity private key corresponding to said identity public key according to said first public/private key encryption algorithm;

comparing said source test data with said resultant test data, said comparing step being performed by said service provider; and

depending on the results of said step of comparing said source test data with said resultant test data, generating an updated descriptor, said updated descriptor comprising said identity public key, updated attribute data, and a digital signature of said identity public key and said updated attribute data.

29. The method for updating attribute data of claim 28, wherein said step of generating an updated descriptor comprises generating said digital signature by encrypting a derivation of said identity public key and said updated attribute data according to a second public/private key encryption algorithm using a signature private key.

30. The method for updating attribute data of claim 28, wherein said request to update attribute data includes old attribute data and an old digital signature, said old digital signature representing an encryption of data derived from said identity public key and said old attribute data, said encryption being according to a second public/private key encryption algorithm using a signature private key, said method further comprising:

decrypting said old digital signature according to said second public/private key encryption algorithm using a signature public key;

comparing the decrypted old digital signature to said data derived from said identity public key and said old attribute data to verify said attribute data;

wherein said step of generating an updated descriptor further depends on the results of said step of comparing the decrypted old digital signature to said data derived for said identity public key and said old attribute data.

31. The method for updating attribute data of claim 28, wherein said first of said pair of complementary data transformations is an encryption of said source test data and said second of said pair of complementary data transformations is a decryption of said source test data encrypted by said first transformation, said first transformation being performed before said second transformation.

32. The method for updating attribute data of claim 28, wherein said second of said pair of complementary data transformations is an encryption of said source test data and said first of said pair of complementary data transformations is a decryption of said source test data encrypted by said second transformation, said second transformation being performed before said first transformation.

33. The method for updating attribute data of claim 28, wherein said service provider is remote from said tangible object.

34. The method for updating attribute data of claim 33, wherein said tangible object is coupled to a local device, said local device communicating remotely with said service provider.

35. The method for updating attribute data of claim 28, further comprising the step of accessing a database in said service provider to verify that the requestor is entitled to the requested update.

36. The method for updating attribute data of claim 28, wherein said source test data is randomly generated data.

37. A method for using verified information concerning a tangible object, comprising the steps of:

accessing descriptor data associated with the tangible object, said descriptor data including an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing information concerning said tangible object, and a digital signature, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data according to a derivation algorithm, said encryption being according to a second public/private key encryption algorithm using a signature private key;

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

deriving data from said identity public key and said attribute data using said derivation algorithm;

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data according to said derivation algorithm;

generating random source test data;

performing a pair of complementary data transformations of said source test data to produce resultant test data, including:

(a) performing a first data transformation of said pair of complementary data transformations according to said first public/private key encryption algorithm using said identity public key, and

(b) accessing a digital protection system attached to said tangible object to perform a second data transformation of said pair of complementary data transformations, said second data transformation being according to said first public/private key encryption algorithm using an identity private key in said digital protection system, said identity private key corresponding to said identity public key according to said first public/private key encryption algorithm;

comparing said random source test data with said resultant test data; and

using said attribute data in a manner dependent on the results of said step of

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data, and said step of comparing said random source test data with said resultant test data.

38. The method for using verified information concerning a tangible object of claim 37, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation..

39. The method for using verified information concerning a tangible object of claim 37, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

40. The method for using verified information concerning a tangible object of claim 37, wherein said step of accessing descriptor data comprises obtaining said descriptor data from said digital protection system.

41. The method for using verified information concerning a tangible object of claim 37, wherein said derivation algorithm comprises a hash function.

42. The method for using verified information concerning a tangible object of claim 41, wherein said hash function belongs to the set consisting of SHA-1 and MD5.

43. The method for using verified information concerning a tangible object of claim 37, wherein said digital protection system is implemented in digital logic contained on a single integrated circuit substrate.

44. An apparatus for verifying information concerning a tangible object, comprising:

a programmable processor;

a memory for storing instructions executable on said programmable processor;

a digital protection system interface coupled to said processor, said interface communicating with a digital protection system for said tangible object;

a protection system verification program executable on said programmable processor, wherein said protection system verification program

(a) obtains a data descriptor from a said digital protection system through said interface, said data descriptor comprising an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing information concerning said object, and a digital signature;

(b) verifies that said digital signature matches said identity public key and said attribute data;

(c) performs a first data transformation of a pair of complementary data transformations of source test data which produce resultant test data, said first data transformation being according to said first public/private key encryption algorithm using said identity public key;

(d) directs said digital protection system to perform a second data transformation of said pair of complementary data transformations of source test data which produce resultant test data, said second data transformation being complementary to said first data transformation;

(e) compares said source test data with said resultant test data; and

(f) verifies information concerning the tangible object responsive to steps (b) and (e).

45. The apparatus for verifying information concerning a tangible object of claim 44, wherein said digital protection system interface is a physical coupling which supplies power to said digital protection system.

46. The apparatus for verifying information concerning a tangible object of claim 44, wherein said digital protection system interface is a remote transmission interface.

47. The apparatus for verifying information concerning a tangible object of claim 44, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data according to a derivation algorithm, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein said protection system verification program verifies that said digital signature matches said identity public key and said attribute data by:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

deriving data from said identity public key and said attribute data using said derivation algorithm; and

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data according to said derivation algorithm.

48. The apparatus for verifying information concerning a tangible object of claim 44, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation..

49. The apparatus for verifying information concerning a tangible object of claim 44, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

50. The apparatus for verifying information concerning a tangible object of claim 44, wherein said source test data is randomly generated data.

51. A method for verifying the identity of a tangible object, comprising the steps of:

accessing a descriptor associated with the tangible object, said descriptor including an identity public key for transforming data according to a first public/private key encryption algorithm;

providing source test data;

performing a pair of complementary data transformations on said source test data to produce resultant test data, said pair of complementary data transformations being performed by:

(a) performing a first data transformation according to said first public/private key encryption algorithm using said identity public key, and

(b) accessing a digital protection system attached to said tangible object to perform a second data transformation according to said first public/private key encryption algorithm using an identity private key in said digital protection system, said identity private key corresponding to said identity public key according to said first public/private key encryption algorithm, said second data transformation being complementary to said first data transformation;

comparing said source test data with said resultant test data; and

using said descriptor to identify said tangible object dependent on the results of said step of comparing said source test data with said resultant test data.

52. The method for verifying the identity of a tangible object of claim 51, wherein said step of using said descriptor to identify said tangible object comprises using said public identity key to access identifying information in a database.

53. The method for verifying the identity of a tangible object of claim 51, wherein said descriptor comprises attribute data and a digital signature of said identity public key and said attribute data, and wherein said step of using said descriptor to identify said tangible object comprises using said attribute data to identify said tangible object if said digital signature matches said identity public key and said attribute data.

54. The method for verifying the identity of a tangible object of claim 51, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation..

55. The method for verifying the identity of a tangible object of claim 51, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

56. A method for providing telephone service, comprising the steps of:

transmitting an identity public key from a telephone to a service provider;

providing source test data, said step of providing source test data being performed by said service provider;

performing a pair of complementary data transformations of said source test data to produce resultant test data, by:

(a) performing a first data transformation of said pair of complementary data transformations according to a first public/private key encryption algorithm using said identity public key, said performing a first data transformation step being performed by said service provider, and

(b) requesting said telephone to perform a second data transformation of said pair of complementary data transformations according to said first public/private key encryption algorithm using an identity private key stored in said telephone, and receiving the results of said second data transformation;

comparing said source test data to said resultant test data, said comparing step being performed by said service provider;

providing service to said telephone depending on whether said source test data matches said resultant test data.

57. The method for providing telephone service of claim 56, further comprising the steps of:

transmitting, from said telephone to said service provider, attribute data and a digital signature of said identity public key and said attribute data;

verifying that said digital signature matches said identity public key and said attribute data; and

providing service to said telephone depending on whether said digital signature matches said identity public key and said attribute data.

58. The method for providing telephone service of claim 57, wherein said digital signature representing an encryption of data derived from said identity public key and said attribute data, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein said step of verifying that said digital signature matches said identity public key and said attribute data comprises:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

comparing the decrypted digital signature to said data derived from said identity public key and said attribute data to verify said attribute data..

59. The method for providing telephone service of claim 57, wherein said attribute data includes an identifier identifying said telephone.

60. The method for providing telephone service of claim 59, wherein said identifier comprises a telephone number of said telephone.

61. The method for providing telephone service of claim 56, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation..

62. The method for providing telephone service of claim 56, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

63. The method for providing telephone service of claim 56, wherein said telephone is a cellular telephone.

64. The method for providing telephone service of claim 56, wherein said source test data is randomly generated data.

65. A telephone, comprising:

a transceiver for communicating with a service provider;

a telephonic interface for audible communication with a user;

an identity public key and corresponding identity private key according to a first public/private key encryption algorithm;

a digital controller controlling the operation of said telephone, wherein said controller:

(a) causes said telephone to transmit said identity public key to a service provider with a request for service;

(b) responsive to a request from said service provider, performs a data transformation of test data received from said service provider according to said first public/private key encryption algorithm using said identity private key; and

(c) transmits the transformed test data to said service provider.

66. The telephone of claim 65, further comprising a digital protection system, said digital protection system comprising:

(a) an external interface for receiving data requests;

(b) an internal processor coupled to said external interface, said processor capable of performing said data transformation according to said first public/private key encryption algorithm; and

(c) an internal data storage;

wherein said identity private key is stored in said internal data storage within said digital protection system, said identity private key being inaccessible outside said external interface to said digital protection system.

67. The telephone of claim 66, wherein said digital protection system is implemented in digital logic contained on a single integrated circuit substrate.

68. The telephone of claim 65, further comprising attribute data and a digital signature of said attribute data and said identity public key, wherein said digital controller further causes said telephone to transmit said attribute data and said digital signature to said service provider with a request for service.

69. The telephone of claim 68, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data, said encryption being according to a second public/private key encryption algorithm using a signature private key.

70. The telephone of claim 68, wherein said attribute data includes an identifier identifying said telephone.

71. A method in a telephone service provider for updating attribute data contained in a telephone, comprising the steps of:

obtaining a descriptor associated with said telephone, said descriptor including an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data, and a digital signature;

verifying that said digital signature matches said attribute data and said identity public key;

performing a pair of complementary data transformations of source test data to produce resultant test data, a first of said pair of complementary data transformations being performed by said service provider according to said first public/private key encryption algorithm using said identity public key, and a second of said pair of complementary data transformations being performed by requesting said telephone to perform said second data transformation according to said first public/private key encryption algorithm using an identity private key in said telephone and receiving data from said telephone responsive to said request, said identity private key corresponding to said identity public key according to said first public/private key encryption algorithm;

comparing said source test data with said resultant test data;

depending on the results of said step of comparing said source test data with said resultant test data, generating an updated descriptor, said updated descriptor comprising said identity public key, updated attribute data, and a digital signature of said identity public key and said updated attribute data; and

transmitting said updated descriptor to said telephone.

72. The method in a telephone service provider for updating attribute data contained in a telephone of claim 71, wherein said step of generating an updated descriptor comprises generating said digital signature by encrypting a derivation of said identity public key and said updated attribute data according to a second public/private key encryption algorithm using a signature private key.

73. The method in a telephone service provider for updating attribute data contained in a telephone of claim 71, wherein said first of said pair of complementary data transformations is an encryption of said source test data and said second of said pair of complementary data transformations is a decryption of said source test data encrypted by said first transformation, said first transformation being performed before said second transformation.

74. The method in a telephone service provider for updating attribute data contained in a telephone of claim 71, wherein said second of said pair of complementary data transformations is an encryption of said source test data and said first of said pair of complementary data transformations is a decryption of said source test data encrypted by said second transformation, said second transformation being performed before said first transformation.

75. The method in a telephone service provider for updating attribute data contained in a telephone of claim 71, wherein said source test data is randomly generated data.

76. The method in a telephone service provider for updating attribute data contained in a telephone of claim 71, wherein said telephone is a cellular telephone.

77. A machine having multiple parts, comprising:

a first replaceable part

a digital controller controlling operation of at least one function of said machine, said digital controller being external to said first replaceable part;

a digital protection system attached to said first replaceable part, said digital protection system comprising:

(a) an external interface for receiving data requests,

(b) a processor coupled to said external interface, said processor capable of performing a first data transformation according to a first public/private key encryption algorithm, and

(c) an internal data storage, said internal data storage storing an identity private key, said identity private key being inaccessible outside said external interface; and

a data descriptor associated with said digital protection system, said data descriptor including an identity public key, attribute data and a digital signature;

wherein said controller verifies information concerning said first replaceable part by:

(a) obtaining said data descriptor associated with said digital protection system,

(b) performing a second data transformation of test data according to said first public/private key encryption algorithm using said identity public key, said second data transformation being complementary to said first data transformation,

(c) accessing said digital protection system attached to said first replaceable part to perform said first data transformation of said test data using said identity private key,

(d) comparing data undergoing said first and second data transformations to test data before transformation; and

(e) verifying that said data descriptor has not been altered using said digital signature.

78. The machine of claim 77, wherein said digital signature is an encryption of data derived from said identity public key and attribute data, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein said controller verifies that said data descriptor has not been altered by:

(e1) decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key, and

(e2) comparing the decrypted digital signature to data derived from said identity public key and said attribute data according to said derivation algorithm to verify said descriptor data..

79. The machine of claim 77, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation..

80. The machine of claim 77, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

81. The machine of claim 77, wherein said apparatus comprises a plurality of replaceable parts, at least some of which contain a respective digital protection system.

82. The machine of claim 81, wherein said machine is a motor vehicle.

83. The machine of claim 77, wherein said digital protection is implemented in digital logic contained on a single integrated circuit substrate.

84. The machine of claim 83, wherein said data descriptor is stored in said internal data storage contained on said single integrated circuit substrate.

85. The machine of claim 84, wherein said data descriptor contains a unique machine identifier, said unique machine identifier distinguishing said machine from other machines of the same type.

86. A replaceable part for a machine having multiple parts, comprising:

a part performing a function for said machine, and

a digital protection system attached to said part, said digital protection system comprising:

(a) an external interface for communicating with a digital controller of said machine, said digital controller being located externally to said replaceable part;

(b) a processor coupled to said external interface, said processor capable of performing a data transformation according to a first public/private key encryption algorithm, and

(c) an internal data storage, said internal data storage storing an identity private key, said identity private key being inaccessible outside said external interface, and a data descriptor, said data descriptor including an identity public key, attribute data and a digital signature;

wherein, responsive to a request received through said external interface, said processor of said digital protection system performs said data transformation according to said first public/private key encryption algorithm using said identity private key.

87. The machine of claim 86, wherein said machine is a motor vehicle.

88. The replaceable part for a machine having multiple parts of claim 86, wherein said digital signature is an encryption of data derived from said identity public key and attribute data, said encryption being according to a second public/private key encryption algorithm using a signature private key, said digital signature being capable of decoding according to said second public/private key encryption algorithm using a signature public key.

89. The replaceable part for a machine having multiple parts of claim 88, wherein said digital signature is an encryption of data derived from said identity public key and attribute data by performing a pre-defined hash function.

90. The machine of claim 86, wherein said digital protection system is implemented in digital logic contained on a single integrated circuit substrate.

91. A method of operating a machine having multiple parts, including a first replaceable part having a digital protection system and a digital controller external to said first replaceable part for controlling operation of said machine, said method comprising the steps of:

(a) obtaining a data descriptor associated with said first replaceable part, said data descriptor including an identity public key, attribute data, and a digital signature;

(b) performing a complementary pair of data transformations of source test data to produce resultant test data, including a first data transformation performed by said digital controller according to a first public/private key encryption algorithm using said identity public key, and a second data transformation performed by said digital protection system, said second data transformation being complementary to said first data transformation;

(c) comparing said source test data to said resultant test data;

(d) verifying that said data descriptor has not been altered using said digital signature; and

(e) using the results of steps (c) and (d) in the operation of said machine.

92. The method of operating a machine of claim 91, wherein step (e) comprises presenting information derived from the results of steps (c) and (d) to a user.

93. The method of operating a machine of claim 91, wherein step (e) comprises selectively disabling at least one function of said machine responsive to the results of steps (c) and (d).

94. The method of operating a machine of claim 91, wherein said data descriptor contains a unique machine identifier, said unique machine identifier distinguishing said machine from other machines of the same type, said method further comprising the step of verifying that said unique machine identifier in said data descriptor matches a unique machine identifier associated with said machine.

95. The method of operating a machine of claim 91, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation.

96. The method of operating a machine of claim 91, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

97. A personal identity document for a subject, comprising:

a carrier; and

a digital protection system attached to said carrier, said digital protection system comprising:

(a) an external interface for receiving data requests,

(b) a processor coupled to said external interface, said processor capable of performing a data transformation according to a first public/private key encryption algorithm, and

(c) an internal data storage, said internal data storage storing an identity private key and a data descriptor, said identity private key being inaccessible outside said external interface, said data descriptor including an identity public key, attribute data and a digital signature of said identity public key and said attribute data, said identity public key corresponding to said identity private key according to said first public/private key encryption algorithm;

wherein said processor performs said data transformation of data responsive to a request received through said external interface, said processor performing said data transformation according to said first public/private key encryption algorithm using said identity private key.

98. The personal identity document of claim 97, wherein said attribute data comprises data identifying a digitized photographic image of said subject.

99. The personal identity document of claim 97, wherein said attribute data comprises data identifying said subject according to at least one physical characteristic verified by a digital data processing device.

100. The personal identity document of claim 99, wherein said data identifying a person according to at least one physical characteristic comprises data derived from an iris scan.

101. The personal identity document of claim 99, wherein said data identifying a person

according to at least one physical characteristic comprises data derived from an retina scan.

102. The personal identity document of claim 99, wherein said data identifying a person according to at least one physical characteristic comprises data derived from a voice sample.

103. The personal identity document of claim 97, wherein said digital signature is an encryption of data derived from said identity public key and attribute data, said encryption being according to a second public/private key encryption algorithm using a signature private key, said digital signature being capable of decoding according to said second public/private key encryption algorithm using a signature public key.

104. The personal identity document of claim 103, wherein said digital signature is an encryption of data derived from said identity public key and attribute data by performing a pre-defined hash function.

105. The apparatus of claim 97, wherein said digital protection system is implemented in digital logic contained on a single integrated circuit substrate.

106. A control station for verifying the personal identities of multiple subjects, comprising:

a programmable processor;

a memory, said memory storing a control program which executes on said programmable processor and controls at least some operations of said control station;

a digital personal identity document interface, said interface communicating with a digital personal identity document of a subject;

wherein said control program verifies a personal identity of a subject by:

(a) obtaining a data descriptor from said digital personal identity document of the subject through said interface, said descriptor comprising an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing identifying information concerning said subject, and a digital signature;

(b) verifying that said digital signature matches said identity public key and said attribute data;

(c) performing a pair of complementary data transformations of source test data to produce resultant test data, said pair of complementary data transformations including (i) a first data transformation according to said first public/private key encryption algorithm using said identity public key, said first data transformation being performed externally to said digital personal identity document, and (ii) a second data transformation according to said first public/private key encryption algorithm, said second data transformation being performed by said digital personal identity document responsive to a request by said control program;

(d) comparing said source test data with said resultant test data; and

(e) verifying the identity of said subject depending on the results of said step of verifying that said digital signature matches said identity public key and said attribute data, and said step of comparing said source test data with said resultant test data.

107. The control station for verifying the identities of multiple subjects of claim 106, wherein said control station is a passport control station at a jurisdictional entry or exit location.

108. The control station for verifying the identities of multiple subjects of claim 106, further comprising an operator interface displaying information to an operator, said information including a result of steps (b) and (d).

109. The control station for verifying the identities of multiple subjects of claim 108, wherein said information displayed to said operator further comprises at least some identifying information derived from said attribute data..

110. The control station for verifying the identities of multiple subjects of claim 109, wherein said identifying information derived from said attribute data comprises a digitized photographic image of said subject.

111. The control station for verifying the identities of multiple subjects of claim 106, further comprising a physical characteristic sensing device, said physical characteristic sensing device automatically sensing at least one physical characteristic of the subject, said at least one physical characteristic being compared to identifying data contained in said data descriptor to verify the identity of said subject.

112. The control station for verifying the identities of multiple subjects of claim 111, wherein said physical characteristic sensing device is an iris scanning device.

113. The control station for verifying the identities of multiple subjects of claim 106, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data according to a derivation algorithm, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein said control program verifies that said digital signature matches said identity public key and said attribute data by:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

deriving data from said identity public key and said attribute data using said derivation algorithm; and

comparing the decrypted digital signature to the data derived from said identity public key and said attribute data according to said derivation algorithm.

114. The control station for verifying the identities of multiple subjects of claim 106, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation.

115. The control station for verifying the identities of multiple subjects of claim 106, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

116. The control station for verifying the identities of multiple subjects of claim 106, wherein said source test data is randomly generated data.

117. A method for verifying the identity of a subject, comprising the steps of:

(a) obtaining a data descriptor from a digital personal identity document of the subject, said descriptor comprising an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data containing identifying information concerning said subject, and a digital signature;

(b) verifying that said digital signature matches said identity public key and said attribute data;

(c) performing a pair of complementary data transformations of source test data to produce resultant test data, wherein a first data transformation of said pair is performed by a verifying device according to said first public/private key encryption algorithm using said identity public key, and wherein a second data transformation of said pair is performed by said digital personal identity document responsive to a request from a verifying device, said second data transformation being complementary to said first data transformation;

(d) comparing said source test data with said resultant test data; and

(e) verifying the identity of said subject responsive to the results of steps (b) and (d).

118. The method for verifying the identity of a subject of claim 117, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data according, said encryption being according to a second public/private key encryption algorithm using a signature private key, and wherein step (b) comprises the steps of:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key;

comparing the decrypted digital signature to said data derived from said identity public key and said attribute data.

119. The method for verifying the identity of a subject of claim 118, wherein said digital signature is an encryption of data derived from said identity public key and attribute data by performing a pre-defined hash function.

120. The method for verifying the identity of a subject of claim 117, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation..

121. The method for verifying the identity of a subject of claim 117, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

122. The method for verifying the identity of a subject of claim 117, further comprising the step of displaying information to an operator, said information including a result of step (e).

123. The method for verifying the identity of a subject of claim 122, wherein said information displayed to said operator further comprises at least some identifying information derived from said attribute data..

124. The method for verifying the identity of a subject of claim 123, wherein said identifying information derived from said attribute data comprises a digitized photographic image of said subject.

125. The method for verifying the identity of a subject of claim 117, further comprising the steps of:

automatically sensing at least one physical characteristic of the subject with a sensing device; and

automatically comparing said at least one physical characteristic to identifying data contained in said data descriptor to verify the identity of said subject.

126. The method for verifying the identity of a subject of claim 125, wherein said sensing device is an iris scanning device.

127. The method for verifying the identity of a subject of claim 117, wherein said source test data is randomly generated data.

128. A method for providing television service to a subscriber, comprising the steps of:

accessing descriptor data in a television receiving apparatus, said descriptor data including an identity public key for transforming data according to a first public/private key encryption algorithm, attribute data and a digital signature of said descriptor data;

verifying that said descriptor data has not been altered using said digital signature;

providing source test data;

performing a first data transformation of a pair of data transformations of said source test data, said pair of data transformations producing resultant test data, said first data transformation being according to said first public/private key encryption algorithm using said identity public key;

requesting a digital protection system of said television receiving apparatus to perform a second data transformation of said pair of data transformations of said source test data, said digital protection system including

(a) a processor capable of performing said second data transformation according to a first public/private key encryption algorithm; and

(b) a permanent data storage accessible only through said processor, said permanent data storage storing an identity private key for performing said second data transformation according to said first public/private key encryption algorithm;

comparing said source test data with the resultant test data to verify the identity of said digital protection system; and

using said attribute data to access one or more television channels on behalf of said subscriber depending on the results of said verifying step and said comparing step.

129. The method for providing television service of claim 128, wherein said attribute data comprises keys for accessing a plurality of channel signals.

130. The method for providing television service of claim 129, wherein said keys for accessing a plurality of channel signals are encrypted.

131. The method for providing television service of claim 128, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data, said encryption being according to a second public/private key encryption algorithm using a signature private key, said verifying step comprising:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key; and

comparing the decrypted digital signature to said data derived from said identity public key and said attribute data to verify said descriptor data.

132. The method for providing television service of claim 128, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation..

133. The method for providing television service of claim 128, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.

134. A television receiving system, comprising:

a digital controller controlling the operation of said television system;

a television signal transmission interface coupled to said digital controller, said interface receiving televisions signals from an external source and transmitting television signals to a display apparatus;

a digital protection system coupled to said digital controller, said digital protection system securely storing an identity private key, and said digital protection system performing a first data transformation according to a first public/private key encryption algorithm in response to a command from said digital controller;

a data descriptor associated with said digital protection system, said data descriptor including an identity public key for performing data transformations according to said first public/private key encryption algorithm, attribute data and a digital signature;

wherein said controller:

(a) directs said digital protection system to perform said first data transformation of test data;

(b) performs a second data transformation of test data according to said first public/private key encryption algorithm using said identity public key;

(c) compares test data before transformation with test data after said first and said second transformation,

(d) verifies that said digital signature matches said identity public key, and

(e) uses said attribute data to access television channels on behalf of a user responsive to the results of steps (c) and (d).

135. The television receiving system of claim 134, wherein said television signal transmission interface receives television signals from a satellite receiver.

136. The television receiving system of claim 134, wherein said attribute data comprises keys for accessing a plurality of channel signals.

137.. The television receiving system of claim 136, wherein said keys for accessing a plurality of channel signals are encrypted.

138. The television receiving system of claim 134, wherein said digital signature represents an encryption of data derived from said identity public key and said attribute data, said encryption being according to a second public/private key encryption algorithm using a signature private key, said verifying step comprising:

decrypting said digital signature according to said second public/private key encryption algorithm using a signature public key; and

comparing the decrypted digital signature to said data derived from said identity public key and said attribute data to verify said descriptor data.

139. The television receiving system of claim 134, wherein said first data transformation is an encryption of said source test data and said second data transformation is a decryption of said source test data encrypted by said first data transformation, said first data transformation being performed before said second data transformation.

140. The television receiving system of claim 134, wherein said second data transformation is an encryption of said source test data and said first data transformation is a decryption of said source test data encrypted by said second data transformation, said second data transformation being performed before said first data transformation.